UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/856,813	08/21/2001	John Desborough Yesburg	1376-010862	3464

7590 11/05/2004

Webb Ziesenheim Logsdon
Orkin & Hanson
700 Koppers Building
436 Seventh Avenue
Pittsburgh, PA 15219-1818

EXAMINER	
COLIN, CARL G	

ART UNIT	PAPER NUMBER
2136	

DATE MAILED: 11/05/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/856,813	YESBURG, JOHN DESBOROUGH	
	Examiner	Art Unit	
	Carl Colin	2136	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
- Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *21 August 2001* .

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-23* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-23* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☒ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *21 August 2001* is/are: a)☐ accepted or b)☒ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

11)☐ The proposed drawing correction filed on _____ is: a)☐ approved b)☐ disapproved by the Examiner.

If approved, corrected drawings are required in reply to this Office action.

12)☐ The oath or declaration is objected to by the Examiner.

Priority under 35 U.S.C. §§ 119 and 120

13)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☒ All b)☐ Some * c)☐ None of:

1.☒ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____ .

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

14)☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. § 119(e) (to a provisional application).

a) ☐ The translation of the foreign language provisional application has been received.

15)☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. §§ 120 and/or 121.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449) Paper No(s) *6* .
4) ☐ Interview Summary (PTO-413) Paper No(s). _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other:

DETAILED ACTION

1. In response to a Pre-Amendment filed on 8-21-2001, the amendment to the specification has been considered. Applicant pre-amends claims 3, 15-19, and 21-22 to eliminate the multiple dependencies. Pursuant to USC 131, claims 1-23 are presented for examination.

Specification

2. The abstract of the disclosure is objected to because of the usage of "means" and "said" language. Correction is required. See MPEP § 608.01(b).

Applicant is reminded of the proper language and format for an abstract of the disclosure.

The abstract should be in narrative form and generally limited to a single paragraph on a separate sheet within the range of 50 to 150 words. It is important that the abstract not exceed 150 words in length since the space provided for the abstract on the computer tape used by the printer is limited. The form and legal phraseology often used in patent claims, such as "means" and "said," should be avoided. The abstract should describe the disclosure sufficiently to assist readers in deciding whether there is a need for consulting the full patent text for details.

The language should be clear and concise and should not repeat information given in the title. It should avoid using phrases which can be implied, such as, "The disclosure concerns," "The disclosure defined by this invention," "The disclosure describes," etc.

Drawings

3. The drawings are objected to as failing to comply with 37 CFR 1.84(p)(5) because they do not include the following reference sign(s) mentioned in the description: "cryptographic engine 30". The drawings are objected to as failing to comply with 37 CFR 1.84(p)(4) because reference characters "10, 12, 14, and 16" appear to point to the same part in the drawing of figure 1. Also reference 12, 14, and 16 are pointed to both inside and outside of part 10.

Corrected drawing sheets in compliance with 37 CFR 1.121(d) are required in reply to the Office action to avoid abandonment of the application. Any amended replacement drawing sheet should include all of the figures appearing on the immediate prior version of the sheet, even if only one figure is being amended. The replacement sheet(s) should be labeled "Replacement Sheet" in the page header (as per 37 CFR 1.84(c)) so as not to obstruct any portion of the drawing figures. If the changes are not accepted by the examiner, the applicant will be notified and informed of any required corrective action in the next Office action. The objection to the drawings will not be held in abeyance.

Claim Rejections - 35 USC § 112

4. The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

4.1 Claims 2-7, 20, and 22 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

Claim 2 recites the limitation "said trusted private key" and "said display" on the third line. There is insufficient antecedent basis for this limitation in the claim.

Claims 4 and 5 recite the limitation "said encryption process". There is insufficient antecedent basis for this limitation in the claim.

Claim 7 recites the limitation "said digital private key protection device's private key". There is insufficient antecedent basis for this limitation in the claim.

Claim 20 recites the limitation "said user identification input means". There is insufficient antecedent basis for this limitation in the claim.

Claim 22 recites the limitation "said PKPD". There is insufficient antecedent basis for this limitation in the claim.

Claims 3-6 recite the limitation "a private key protection system according to claim 1". There is insufficient antecedent basis for this limitation in the claim. Claim is referring to a device.

Claim Rejections - 35 USC § 102

5. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(e) the invention was described in a patent granted on an application for patent by another filed in the United States before the invention thereof by the applicant for patent, or on an international application by another who has fulfilled the requirements of paragraphs (1), (2), and (4) of section 371(c) of this title before the invention thereof by the applicant for patent.

The changes made to 35 U.S.C. 102(e) by the American Inventors Protection Act of 1999 (AIPA) and the Intellectual Property and High Technology Technical Amendments Act of 2002 do not apply when the reference is a U.S. patent resulting directly or indirectly from an international application filed before November 29, 2000. Therefore, the prior art date of the reference is determined under 35 U.S.C. 102(e) prior to the amendment by the AIPA (pre-AIPA 35 U.S.C. 102(e)).

5.1 **Claims 1, 4, 10, 12-13, 17-23** is rejected under 35 U.S.C. 102(e) as being anticipated by US Patent 5,917,913 to **Wang**.

5.2 **As per claims 1, 17-23, Wang** discloses a digital private key protection device, comprising a digital private key storage means containing a user's digital private key, for example (see column 9, lines 5-20); a cryptographic engine, for example (see column 9, lines 1-6); a communications port for receiving digital data from an external device, and for transmitting data to said external device, for example (see column 9, lines 20-40); a display means for displaying said received digital data, for example (see column 10, line 65 through column 11, 12); a user operable input means connected to said cryptographic engine to indicate when operated by said user their approval of said displayed received digital data, for example (see column 11, lines 14-41, column 10, lines 36-67); wherein said cryptographic engine is trusted to only apply said user's digital private key to sign said received data only if said user operable input means is operated and communicate said signed data external of said digital private key protection device, for example (see column 11, lines 33-62 and column 4, lines 40-65).

As per claim 4, Wang discloses the limitation of an audit means that meets the recitation of wherein signed data is not transmitted external of said digital private key protection device until a said encryption process is audited by said audit means, for example (see column 7, lines 1-17 and column 12, lines 35-50; column 4, lines 40-55).

As per claim 10, Wang discloses the limitation of wherein said cryptographic engine is trusted to decrypt digital data using said user's digital private key and passing decrypted digital data to said display means for display of said received digital data, for example (see column 7, lines 42-61).

As per claims 12-13, Wang discloses the limitation of wherein said communications port cannot transmit said decrypted digital data unless said user operable input means is operated, for example (see column 4, lines 40-65).

Claim Rejections - 35 USC § 103

6. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

6.1 **Claims 2, 3, 5, 14-16** are rejected under 35 U.S.C. 103(a) as being unpatentable over US Patent 5,917,913 to **Wang** in view of **Bruce Schneier**, Applied Cryptography, 1996, John Wiley & Sons, Second Edition, Pages 43-44.

6.2 **As per claims 2, 3, 5, 14-16, Wang** substantially teaches the claimed method of claim 1 and discloses that the invention is not limited to any encryption scheme, for example (see column 5, lines 35-50). **Wang** discloses that the received data can be encrypted using a trusted public and private key and also discloses a display means for verification of data and approval, for example (see column 7, lines 18-67). **Schneier** in an analogous art teaches a key certification authority wherein the users' public keys are signed with a trusted private key to prevent attack against public key, for example (see pages 43, 62-64); and further discloses validating signature of said user's public key with said trusted public key to determine the veracity of said user's public key and then decrypts said received data using said verified predetermined user's public key, for example (see pages 43, 62-64). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the method of **Wang** to have the public keys signed by a trusted private key using public/private key pairs as taught by **Schneier**. This modification would have been obvious because one skilled in the art would have been motivated by the suggestions provided by **Schneier** so as to prevent attack against public key.

As per claim 5, Wang discloses the limitation of an audit means that meets the recitation of wherein signed data is not displayed until a said encryption process is audited by said audit means, for example (see column 7, lines 1-17 and column 12, lines 35-50).

7. **Claims 6, 7, 8, 9, and 11** are rejected under 35 U.S.C. 103(a) as being unpatentable over US Patent 5,917,913 to **Wang** in view of US Patent 6,408,388 to **Fisher**.

7.1 **As per claim 6, Wang** substantially teaches the claimed method of claim 1 and discloses an input means to secure access of the private key, and input means to perform approval and encryption of the approval, for example (see column 5, lines 18-22). **Wang** does not explicitly disclose using a private key protection device in addition to the user private key. **Fisher** in an analogous art teaches a private key protection device wherein said digital private key protection device further comprises a private key protection device private key storage means wherein digital data signed by said private key protection device is further signed by said private key of said private key protection device for adding more security, for example (see column 8, lines 10-42). Therefore, it would have been obvious to one of ordinary skill in the art of cryptography at the time the invention was made to modify the method of **Wang** to provide a private key protection device wherein said digital private key protection device further comprises a private key protection device private key storage means wherein digital data signed by said private key protection device after operation of said user operable input means is further signed by said private key of said private key protection device as taught **Fisher**. This modification would have been obvious because one skilled in the art would have been motivated by the suggestions provided by **Fisher** so as to add more security.

Claims 7-8 discloses the same inventive concept as discussed in claim 6 except for signing with a public key instead of a private key to verify the corresponding key. This

modification would have been obvious to one of ordinary skill in the art of cryptography to encrypt with either public key or private key to verify the corresponding key, for example (see Fisher, column 6, line 25 through column 7, line 20). (See also Wang, column 42-61). Therefore, claim 7 is rejected on the same rationale as the rejection of claim 6.

Claim 9 discloses the same inventive concept as discussed in claims 6-8. **Fisher** discloses storing plurality of user's public keys, for example (see column 8, lines 42-56; column 11, lines 25-36). Therefore, claim 9 is rejected on the same rationale as the rejection of claims 6-8.

As per claim 11, Wang discloses encryption cannot take place unless said user operable input means is operated. The modification of decryption cannot take place unless said user operable input means is operated does not depart from the spirit and scope of the invention disclosed by **Wang**. See also column 8, lines 18-34. If signed data need to be decrypted by user's private key, said user operable input means needs to be operated.

Conclusion

8. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure as the art protection device to protect private keys of users and several cryptographic schemes to verify signatures and key used. Many of the claimed features are disclosed in these references.

US Patents: 4,529,870 Chaum

4,731,842	Smith
6,212,635	Reardon
6,484,260	Scott et al.

8.1 Any inquiry concerning this communication or earlier communications from the examiner should be directed to Carl Colin whose telephone number is 703-305-0355. The examiner can normally be reached on Monday through Thursday, 8:00-6:30 PM.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on 703-305-9648. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is 703-305-3900.

cc

Carl Colin

Patent Examiner

October 6, 2004

AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100